



Department of the Army Public Key Infrastructure

Gary A. Robison

Information Assurance Directorate

ODISC4, HQDA

11 January 2000



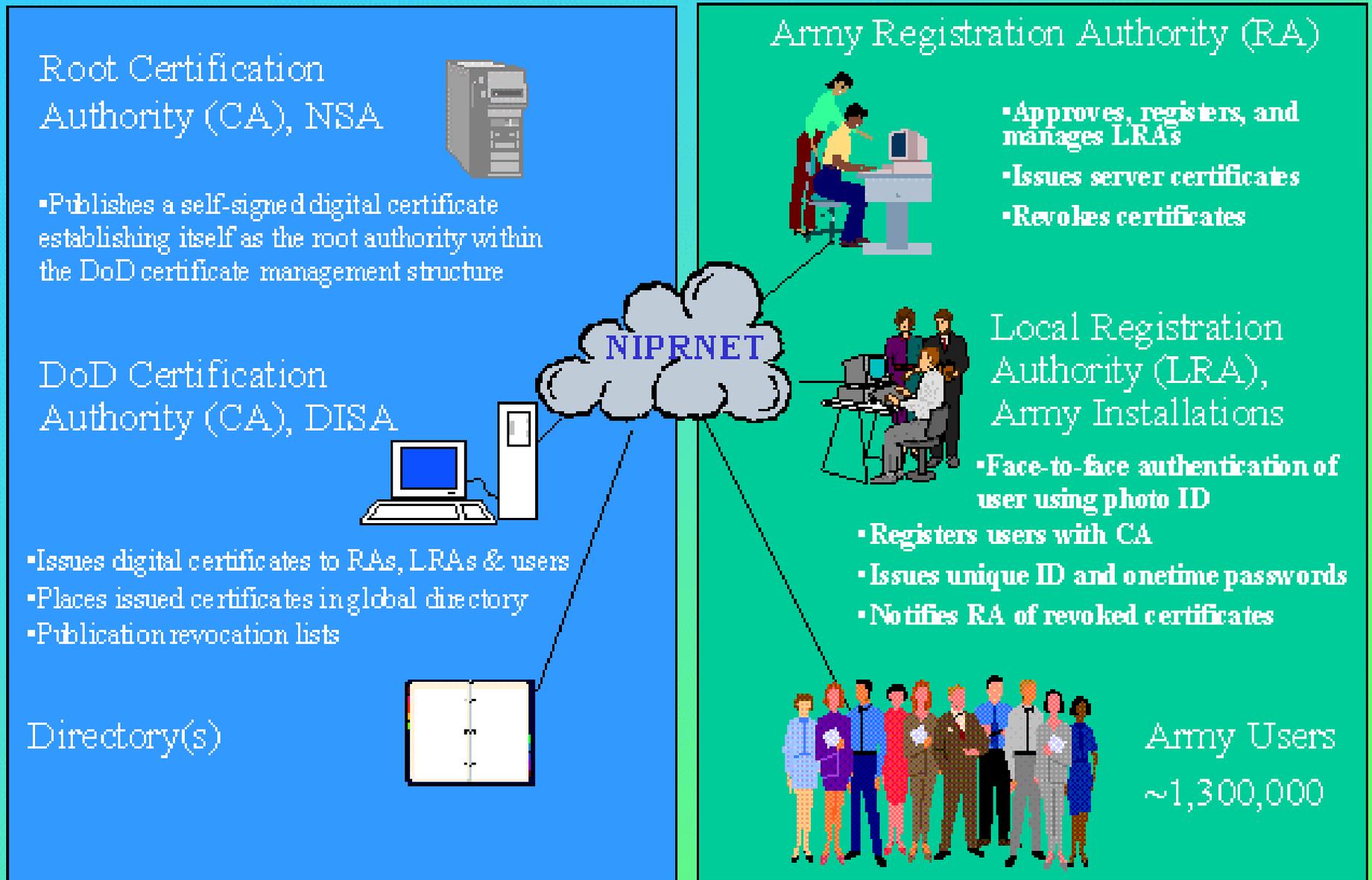
Outline

- What is the Public Key Infrastructure?
- DoD Public Key Infrastructure Architecture
- PKI Status
- Policies
- Overview of DoD PKI Policy Memorandum
 - DoD PKI Milestones
 - PKI Policy Timeline
- Overview of Smart Card Memorandum
- Overview of PKI Enabling of Applications
- Updating DoD PKI Guidance
- Questions/POC

What is the Public Key Infrastructure?

- **The Public Key Infrastructure is that portion of the security management infrastructure dedicated to the management of keys and certificates used by Public Key based security services.**
- **It is a combination of products, services, facilities, policies, procedures, agreements, and people that provides for and sustains secure interactions in open networks.**

DoD Public Key Infrastructure Architecture



PKI Status

- Army Public Key Infrastructure is funded FY00 - FY05
- Army PKI Implementation Plan
- Registration Authorities established and trained
- Validated Requirement for PKI Product Manager
 - Acting Product Manager designated
- DoD PKI Program Manager established
- DoD X.509 Certificate Policy, Ver 5.0 and DoD PKI Roadmap, 29 Oct 1999, Ver 3.0 approved by ASD C3I
- DoD PKI Implementation Plan, 29 Oct 1999, Ver 2.0
- DoD PKI User Requirements, draft, 15 Dec 1999
- USAREUR Medium Grade Messaging Pilot

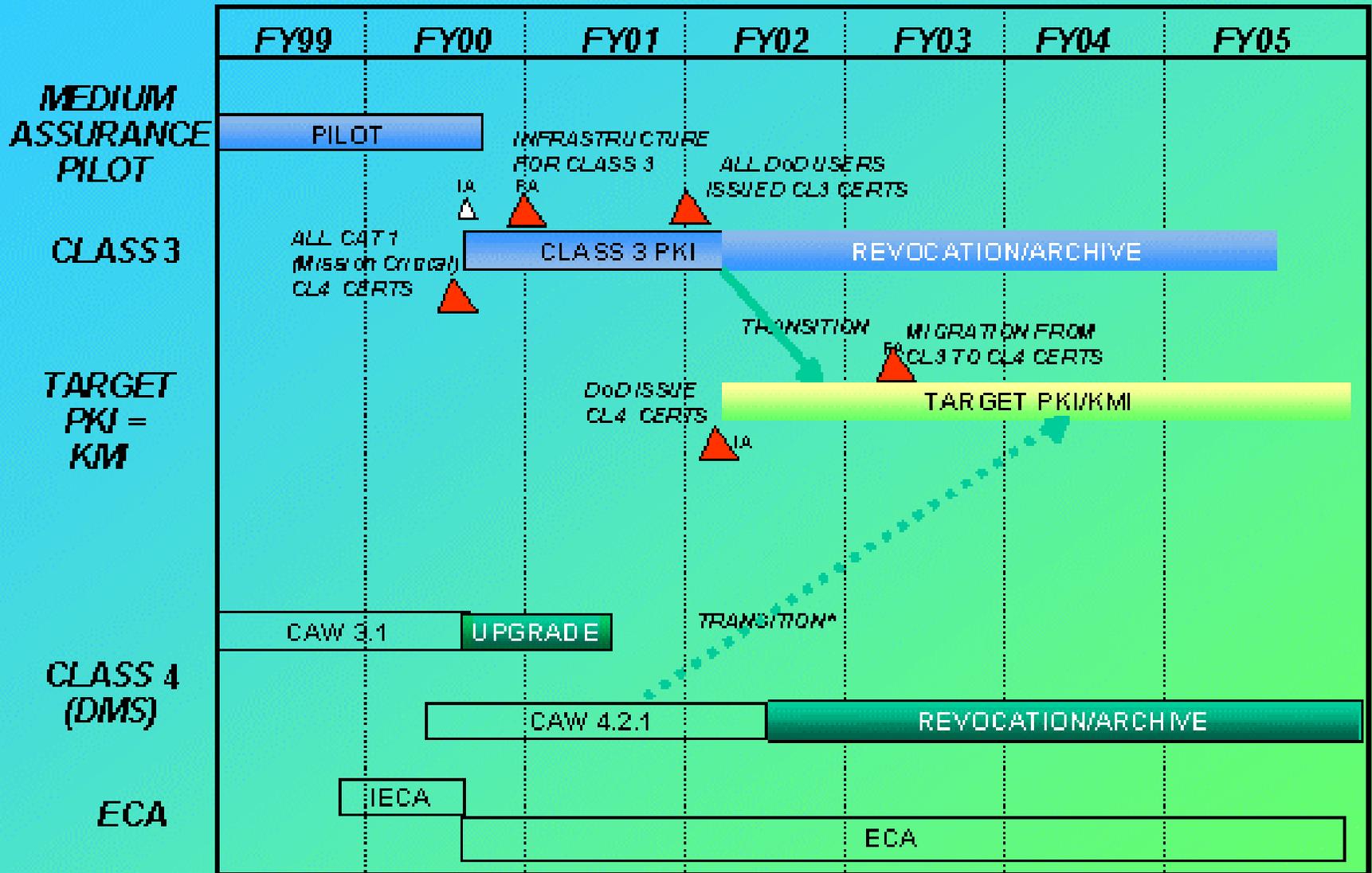
Policies

- DEFSECDEF Memorandum, *Department of Defense (DoD) Public Key Infrastructure (PKI)*, May 6, 1999
- DEFSECDEF Memorandum, *Smart Card Adoption and Implementation*, Nov 10, 1999
- Draft ASD C3I Memorandum, *Public Key Enabling of Applications for the Department of Defense Public Key Infrastructure*, Nov 24, 1999 unsigned
- ASD C3I Memorandum, Public Key Infrastructure (PKI) Operating Documents, Dec 13, 1999

Overview of DoD PKI Policy Memorandum

- **Selection of Appropriate PKI Certificate Assurance Levels**
 - Defined 3 Classes of Certificates (Class 3, Class 4, Class 5)
 - All DoD users will be issued Class 3 certificate by Oct 2001
- **Deployment of PKI Registration Capability**
 - Every DoD organization must deploy registration capability by Oct 2000
- **Evolution of DoD Certificates**
 - Begin to evolve from Class 3 to Class 4 certificates by Jan 2002
- **DoD PKI Certificate Types and Content**
- **External Certificate Authorities**
- **Web Server Access Control via Public Key Techniques**
 - By June 2000 PKI enable all private servers
 - By Oct 2001 require client I&A via Class 3 certificates
- **Signed Electronic Mail**
 - By Oct 2001, all electronic mail will be signed

DoD PKI Milestones



IA = Initial Availability / FA = Final Availability

PKI Policy Timeline

	FY99				FY00				FY01				FY02				FY03				FY04			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
CAT 1 MCS PKI Migrate to Class 4				▲	→	→	→	→	▼															
Private Web Servers issue Class 3				▲	→	→	→	→	▼															
Private Web Servers use Class 3 for server authentication via SSL				▲	→	→	→	→	▼															
Field Capability to issue Class 3				▲	→	→	→	→	▼															
All DoD Users Issued Class 3 PKI				▲	→	→	→	→	→	→	→	→	▼											
Private Web Servers use Class 3 for Client Identification													▼	→	→	→	→	→	→	→	→	→	→	→
Class 3 Signature on all e-mail													▼	→	→	→	→	→	→	→	→	→	→	→
CAT 2 & 3 MCS Migrate to Class 4					▲	→	→	→	→	→	→	→	→	→	→	→	→	→	→	→	▼			
Begin Replacing Class 3 with Class 4																					▼	→	→	→

Overview of Smart Card Memorandum

- **Initial implementation shall be as a DoD-wide common access card**
 - Standard ID card for active duty military, DoD civilians, and eligible contractor personnel
 - Principle card for building access and computer networks and systems
- **Issued and maintained using the Defense Enrollment Eligibility Reporting System and the Real Time Automated Personnel Identification System (DEERS/RAPIDS)**
- **Public Key Certificates to be placed on the common access card**
- **DoD CIO authorized to modify previously issued PKI guidance, as appropriate, to incorporate and accommodate use of the CAC.**
- **Initial implementation no later than Dec 30, 2000**
- **Navy has lead in preparing a smart card Operational Requirements Document**
 - Jan 31, 2000
 - CAC Execution Plan within 120 days

Overview of PKI Enabling of Applications

- All DoD networks and AIS shall be enabled with the capability to control access and authenticate users via DoD PKI Class 4 NLT Dec 31, 2004
- All newly procured applications that use public key technology shall be PK-enabled based on information environment and requirements for digital signature/encryption
- All e-mail applications shall be enabled for digital signature and encryption; all web applications shall be enabled for digital signature and where appropriate and technically feasible, encryption
- All private DoD web servers shall be enabled to use Class 3 certificates for server authentication NLT June 2000.
 - All client applications accessing private DoD web servers shall be enabled to support client/server authentication

Updating Department of Defense Public Key Infrastructure Guidance

- **ASD C3I**
 - DoD PKI Policy Memorandum - underway now
 - DoD Public Key Infrastructure Roadmap
 - Will be updated to incorporate Common Access Card by - April 15, 2000
- **Certificate Policy Management Working Group**
 - DoD X.509 Certificate Policy - update annually
- **DoD PKI PMO**
 - DoD Implementation Plan

QUESTIONS?

POC

Gary A. Robison

DISC4 Information Assurance Office

Gary.Robison@hqda.army.mil

(703) 604-7573

Reminder

- no new certificate infrastructures will be created.
- On going pilots may be continued, but costs should be minimized
- risk management decision must be reviewed